How capture the packet on the firewall

Limitation: a.Currently, this function can only use in the CLI, WebUI is not supported.

b. Not all the firmware version were supported this function.

Purpose: To capture the packet on the firewall, we should use the *pcapdump* command

```
DFL-860:/> pcapdump
Valid options: -cleanup, -show, -start, -status, -stop, -wipe, -write, <enter>
```

Procedure:

1. To start capture the packet on the lan interface we can do the following command:

DFL-860:/> pcapdump -start lan

Starting packet capture on: lan

```
DFL-860:/> pcapdump -start lan
Starting packet capture on: lan
```

You can also capture the other interface

2. Type the following for stop capturing the packet on the lan:

DFL-860:/> pcapdump -stop lan

Stopping packet capture on: lan

```
DFL-860:/> pcapdump -stop lan
Stopping packet capture on: lan
```

3. Put the capturing packet in a file(Test.cap) by typing the following command:

DFL-860:/> pcapdump -write -filename=Test.cap lan

```
DFL-860:/> pcapdump -write -filename=Test.cap lan Dumping capture for lan to "Test.cap"
```

4. Check the Test.cap file is created in the root directory by the following command:

DFL-860:/> ls

OCHEL VALLA OPCION, KENCELZ	
DFL-860:/> pcapdump -write -filename=Test.cap 1	an
Dumping capture for lan to "Test.cap"	
DFL-860:/>ls	
HTTPALGBanners/	
HTTPAuthBanners/	
Test.cap	
certificate/	
config.bak	
full.bak	
script/	
selftest.txt	
sshclientkey/	

How to get the file from the firewall to local PC

[Topology]:

PC(192.168.1.91/24)-----LAN(192.168.1.1/24)DFL-860

[Procedure]:

1. Check the firewall has open the ssh function via the following:

			🟠 🔻 🖾 👻 🗆	🛛 🖶 🔻 Page 🕶 Safety 🕶 T
				Logged in as administr admin - 192.168.1.91
Maintenance 🗸				😚 Logoι
DFL-860 DS Setup and configure methods and permissions for remote management of this system. Add Advanced Settings Matrix Difference				
Туре 🚽	Mode 🚽	Interface 🚽	Network 🚽	Comments 🚽
HTTP/HTTPS Management	Admin: HTTPS	🔝 lan	🗟 lannet	
• 				Right-click on a row for addition
	Maintenance - gement togs Type - HTTP/HTTPS Management	Maintenance gement dots and permissions for remote management of this system. trigs Type Mode HTTP/HTTPS Management Admin: HTTPS	Maintenance • genent totg and pernissions for remote management of this system. tings Type • Mode • Interface • HTTP/HTTPS Management Admin: HTTPS	Maintenance Maint

🔇 🈚 Home 🔰 🔣 Configuration 🗸	🎢 Tools 🗸 🥱 Status 🗸 🔩 Maintenance 🗸
DFL-860 DFL-860 Date and Time DNS DNS Construction Remote Management Dr Log and Event Receivers DhCP Misc. Clients DhCP Whitelist DhCP Whitelist DhCP Digets D	SSH Management Configure a Secure Shell (SSH) Server to enable remote management access to the system. General Image: SSH_enable Listening Port: 22 Max Concurrent Clients: 5 Session idle timeout: 1800 Login grace timeout: 30 Greeting Message:
₽ ig Routing	
DFL-860 Gase and Time Conte and Time Conte and Time Conte Management	AES-128 V Blowfish V AES-192 V 3DES V AES-266 V
Log and Event Receivers Log And Event Receivers Misc. Clients Hardware Monitoring Whitelist	SHA1 ♥ MD5 ♥ SHA1-98 ♥ MD5-98 ♥
Objects Objects Rules Rules Rules Objects	Select the user database to use for login and the access level to grant to the user. User Database: AdminUsers Access Level: Admin Access level Access level Access level Access level
uarigg User Authentication □ - 23 Traffic Management □ - 20 ZoneDefense	Remote access is granted from the following interface and network. Interface: Ian Network: Iannet
	2) Comments

 Download the software PSCP software from the following website since we are using Windows system on the PC:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

3. Check the path of pscp.exe file via the following steps:



pscp.exe Pro	operties	
General Comp	patibility Security Details	
R R R R R R R R R R R R R R R R R R R	pscp.exe	
Type of file: Description:	Application (.exe) Command-line SCP/SFTP client	
Location:	C:\Users\owner\Desktop	
Size:	288 KB (294,912 bytes)	
Size on disk:	288 KB (294,912 bytes)	
Created:	2009年12月30日, 下午 02:14:53	
Modified:	2009年12月30日, 下午 02:14:53	
Accessed:	2009年12月30日, 下午 02:14:53	
Attributes:	Read-only Hidden	Advanced
Security:	This file came from another computer and might be blocked to help protect this computer.	Unblock
	OK Cancel	Apply

4. Copy the location of this software part and open the **command prompt, then change it** to this location like the following:



5. Download the file via the following command:



The syntax is pscp.exe admin_account@Firwall_IP:filename_onfirewall local_PC_filename

6. After you checked the file is downloaded to local PC, you can type the following command to erase the file on the firewall:

```
DFL-860:/> pcapdump -cleanup
PCAPDump cl<u>e</u>aned up.
```